カードベース暗号と論理パズル

岩本貢@電気通信大学大学院情報理工学研究科

離散数学講義資料

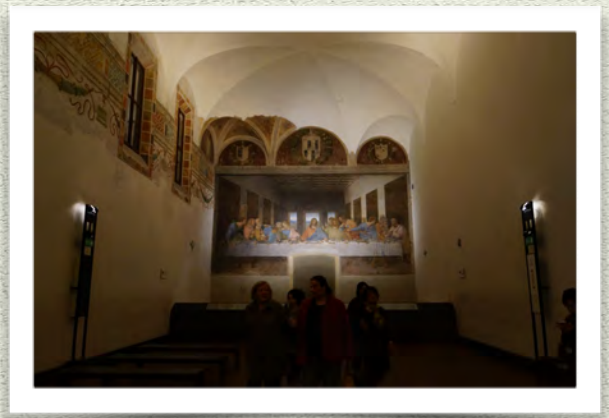
2019 7/23 & 26

はじめに

- ここでご紹介する成果は，2016年度の研究成果
  T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K, Ohta,
  “Efficient Card-based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations,”
  CANS2016, Milan, Nov. 2016. の一部です

はじめに

- ここでご紹介する成果は，2016年度の研究成果
  T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K, Ohta,
  “Efficient Card-based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations,”
  CANS2016, Milan, Nov. 2016. の一部です



はじめに

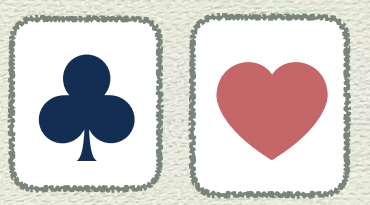
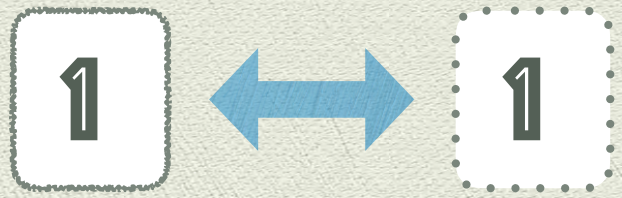
- ここでご紹介する成果は，2016年度の研究成果
  T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K, Ohta,
  “Efficient Card-based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations,”
  CANS2016, Milan, Nov. 2016. の一部です

はじめに

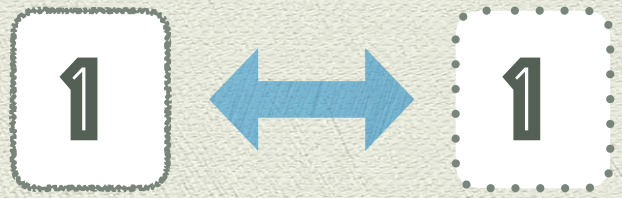
- ここでご紹介する成果は，2016年度の研究成果
  T. Nakai, Y. Misawa, Y. Tokushige, M. Iwamoto, and K, Ohta,
  “Efficient Card-based Cryptographic Protocols for Millionaires’ Problem Utilizing Private Permutations,”
  CANS2016, Milan, Nov. 2016. の一部です



カードベース暗号プロトコル
[B. den Boer, 1989]

- 使うカード：２種類: 
  - 符号化：
    - 0 $\mapsto$  1 $\mapsto$ 
- 暗号化　（隠す）
  - 裏返す：　 
  - 背後での操作（背面操作）：OK

カードベース暗号プロトコル
[B. den Boer, 1989]

- 使うカード：２種類: 
  - 符号化：
    - 0 ↦  1 ↦ 
- 暗号化 （隠す）
  - 裏返す： 
  - 背後での操作（背面操作）：OK

今日の話題：金持ち比べ

- A. C-C Yao (1982)
- 二人の金持ちがどちらがリッチか知りたい
  - どちらも自分の資産を（大小以外）教えたくない
- 技術的には，二者間秘匿計算問題，という

基本的アイデア：
最下位からビット毎に比較

$a = (a_n \cdots a_1)_2$ と $b = (b_n \cdots b_1)_2$ を最下位から比較

単にボブにビットを送る

$a = (0\ 0\ 0)_2$

$a_i \in \{0, 1\}$

$b = (0\ 1\ 0)_2$

基本的アイデア：最下位からビット毎に比較

$a = (a_n \cdots a_1)_2$ と $b = (b_n \cdots b_1)_2$ を最下位から比較

単にボブにビットを送る

$a = (0\ 0\ 0)_2$

$a_i \in \{0, 1\}$

$b = (0\ 1\ 0)_2$

$a_i \neq b_i$ ならば
“Record”をb_iで置き換え

	1st bit	2nd bit	3rd bit
Record	R		

基本的アイデア：最下位からビット毎に比較

$a = (a_n \cdots a_1)_2$ と $b = (b_n \cdots b_1)_2$ を最下位から比較

単にボブにビットを送る

$a = (0\ 0\ 0)_2$

$a_i \in \{0, 1\}$

$b = (0\ 1\ 0)_2$

$a_i \neq b_i$ ならば
“Record”をb_iで置き換え

	1st bit	2nd bit	3rd bit
Record	R		

そのまま

基本的アイデア：最下位からビット毎に比較

$a = (a_n \cdots a_1)_2$ と $b = (b_n \cdots b_1)_2$ を最下位から比較

単にボブにビットを送る

$a = (0\ 0\ 0)_2$

$a_i \in \{0, 1\}$

$b = (0\ 1\ 0)_2$

$a_i \neq b_i$ ならば
“Record”をb_iで置き換え

	1st bit	2nd bit	3rd bit
Record	R	1	
	そのまま	置き換え	

基本的アイデア：
最下位からビット毎に比較

$a = (a_n \cdots a_1)_2$ と $b = (b_n \cdots b_1)_2$ を最下位から比較

単にボブにビットを送る

$a = (0\ 0\ 0)_2$

$a_i \in \{0, 1\}$

$b = (0\ 1\ 0)_2$

$a_i \neq b_i$ ならば
“Record”をb_iで置き換え

	1st bit	2nd bit	3rd bit
Record	R		1
	そのまま	置き換え	そのまま

基本的アイデア：
最下位からビット毎に比較

$a = (a_n \cdots a_1)_2$ と $b = (b_n \cdots b_1)_2$ を最下位から比較

単にボブにビットを送る

$a = (0\ 0\ 0)_2$

$a_i \in \{0, 1\}$

$b = (0\ 1\ 0)_2$

$a_i \neq b_i$ ならば
“Record”をb_iで置き換え

	1st bit	2nd bit	3rd bit
Record	R		1
	そのまま	置き換え	そのまま

改良案：
ダミーカード＆アリスに嘘をつかせる

$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

$a = (0\ 0\ 0)_2$

a_i or $\overline{a_i}$

$b = (0\ 1\ 0)_2$

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

$a = (0\ 0\ 0)_2$

a_i or $\overline{a_i}$

$b = (0\ 1\ 0)_2$

Record

R

Dummy

D

a_i

	1st bit	2nd bit	3rd bit
Record	R		
Dummy	D		

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

$a = (0\ 0\ 0)_2$

a_i or $\overline{a_i}$

$b = (0\ 1\ 0)_2$

Record

R

Dummy

D

a_i

	1st bit	2nd bit	3rd bit
Record	R		
Dummy	0		

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

$a = (0\ 0\ 0)_2$

a_i or $\overline{a_i}$

$b = (0\ 1\ 0)_2$

Record

R

Dummy

D

a_i

	1st bit	2nd bit	3rd bit
Record	R	1	
Dummy	0		

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

$a = (0\ 0\ 0)_2$

a_i or $\overline{a_i}$

$b = (0\ 1\ 0)_2$

Record

R

Dummy

D

a_i

	1st bit	2nd bit	3rd bit
Record	R	1	
Dummy	D	0	

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

$a = (0\ 0\ 0)_2$

a_i or $\overline{a_i}$

$b = (0\ 1\ 0)_2$

Record

R

Dummy

D

a_i

	1st bit	2nd bit	3rd bit
Record	R	1	
Dummy	D	0	0

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

$a = (0\ 0\ 0)_2$

a_i or $\overline{a_i}$

$b = (0\ 1\ 0)_2$

Record

R

Dummy

D

a_i

	1st bit	2nd bit	3rd bit
Record	R		1
Dummy	D	0	0

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

比べようがない！

$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

a_i or $\overline{a_i}$

Record

R

Dummy

D

a_i

	1st bit	2nd bit	3rd bit
Record	R		1
Dummy	D	0	0

改良案：
ダミーカード＆アリスに嘘をつかせる

正直に振る舞うか嘘をつく

比べようがない！

$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

a_i or $\overline{a_i}$

Record

R

Dummy

D

a_i

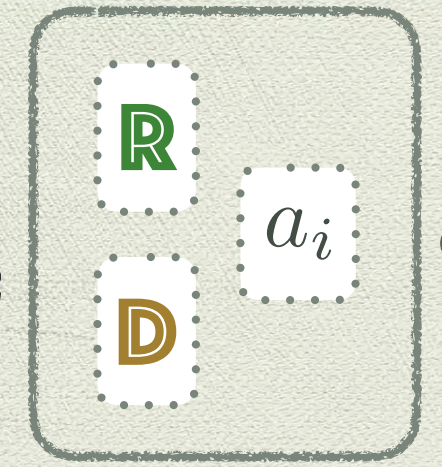
	1st bit	2nd bit	3rd bit
Record	R		1
Dummy	D	0	0

+ もう一工夫（次のスライド）

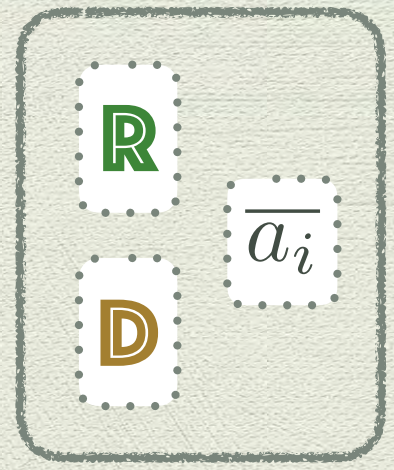
提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$



or

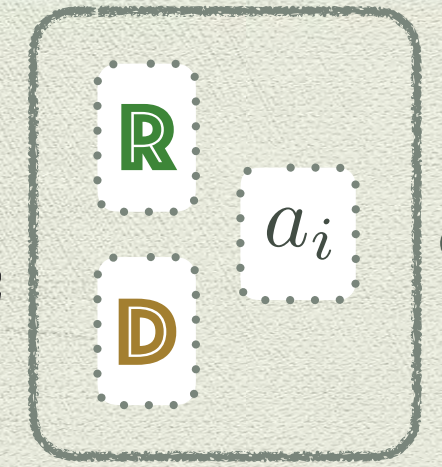


$b = (0\ 1\ 0)_2$

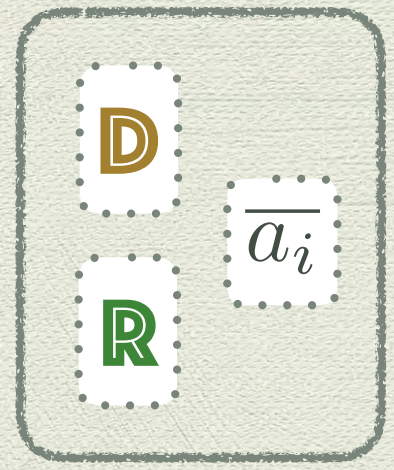
提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$



or



$b = (0\ 1\ 0)_2$

提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはこれを
背面で準備

$a = (0\ 0\ 0)_2$

R
D
a_i

or

D
R
$\overline{a_i}$

$b = (0\ 1\ 0)_2$

提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはこれを
背面で準備

$a = (0\ 0\ 0)_2$

R
D
a_i

or

D
R
$\overline{a_i}$

どちらか知って
いるのはアリスだけ

$b = (0\ 1\ 0)_2$

提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはこれを
背面で準備

$a = (0\ 0\ 0)_2$

R
D
a_i

or

D
R
$\overline{a_i}$

どちらか知って
いるのはアリスだけ

$b = (0\ 1\ 0)_2$

R/D
R/D
$\tilde{a}_i$

提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはこれを
背面で準備

$a = (0\ 0\ 0)_2$

R
D
a_i

or

D
R
$\overline{a_i}$

どちらか知って
いるのはアリスだけ

$b = (0\ 1\ 0)_2$

Top

$\tilde{a}_i \neq b_i$
b_iで置き換え

R/D
R/D
$\tilde{a}_i$

提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはこれを
背面で準備

$a = (0\ 0\ 0)_2$

R
D
a_i

or

D
R
$\overline{a_i}$

どちらか知って
いるのはアリスだけ

$b = (0\ 1\ 0)_2$

Top
$\tilde{a}_i \neq b_i$
b_i で置き換え

Bottom
$\tilde{a}_i = b_i$
b_i で置き換え

R/D
R/D
$\tilde{a}_i$

提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはこれを
背面で準備

$a = (0\ 0\ 0)_2$

R
D
a_i

or

D
R
$\overline{a_i}$

どちらか知って
いるのはアリスだけ

$b = (0\ 1\ 0)_2$

Top/Bottom strategy
ボブは背面で操作
どちらか知っている
のはボブだけ

Top
$\tilde{a}_i \neq b_i$
b_i で置き換え

Bottom
$\tilde{a}_i = b_i$
b_i で置き換え

R/D
R/D
$\tilde{a}_i$

提案プロトコル

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはこれを
背面で準備

$a = (0\ 0\ 0)_2$

R
D
a_i

or

D
R
$\overline{a_i}$

どちらか知って
いるのはアリスだけ

$b = (0\ 1\ 0)_2$

Top/Bottom strategy
ボブは背面で操作
どちらか知っている
のはボブだけ

Top
$\tilde{a}_i \neq b_i$
b_i で置き換え

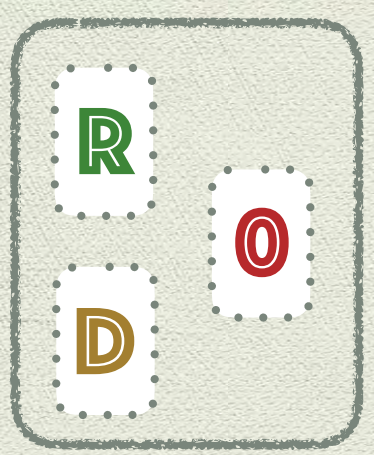
Bottom
$\tilde{a}_i = b_i$
b_i で置き換え

R/D
R/D
$\tilde{a}_i$

プロトコルの実行例：1st Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

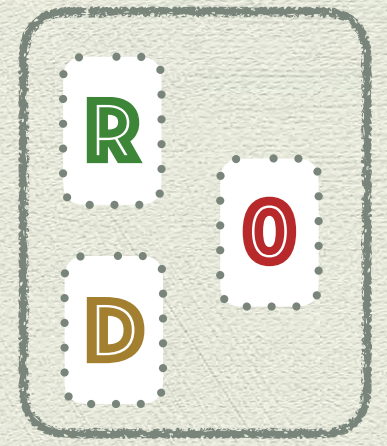


$b = (0\ 1\ 0)_2$

プロトコルの実行例：1st Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

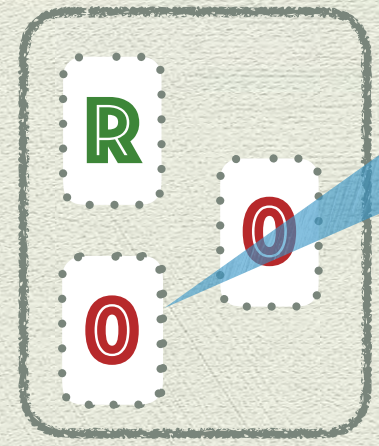


$b = (0\ 1\ 0)_2$

プロトコルの実行例：1st Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$



ボブは Bottom を
0 で置き換える

$b = (0\ 1\ 0)_2$

プロトコルの実行例：1st Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

R

0

プロトコルの実行例：1st Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

R

0

プロトコルの実行例：1st Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

$\mathbb{R}$

0

$b = (0\ 1\ 0)_2$

プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

R

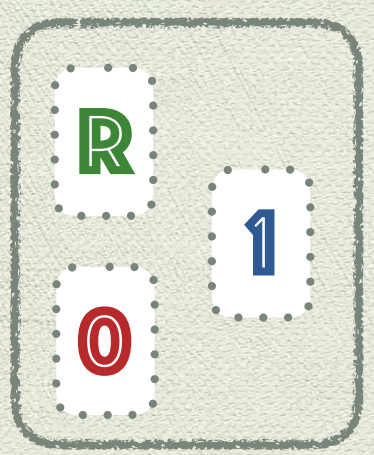
0

$b = (0\ 1\ 0)_2$

プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

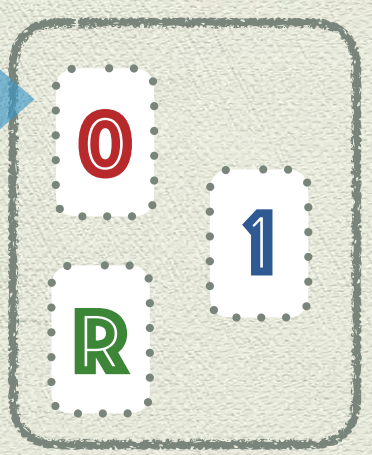


$b = (0\ 1\ 0)_2$

プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

アリスはR/Dを
スワップ



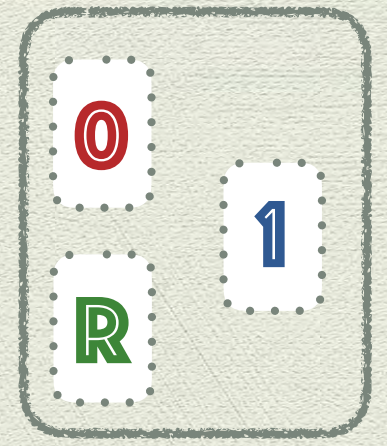
$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

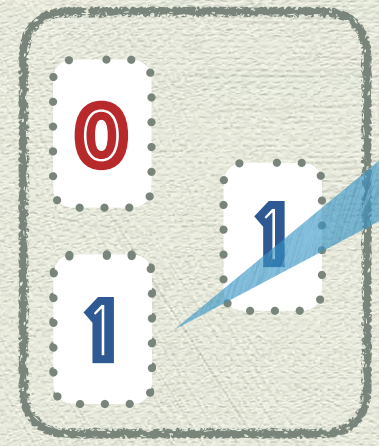


$b = (0\ 1\ 0)_2$

プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$



ボブは Bottom を
1 で置き換える

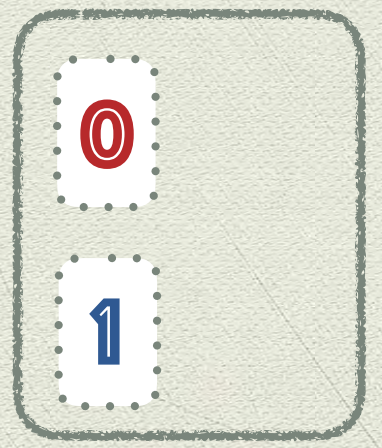
$b = (0\ 1\ 0)_2$

プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$



プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

0

1

プロトコルの実行例：2nd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

0

1

$b = (0\ 1\ 0)_2$

プロトコルの実行例：3rd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

D 0

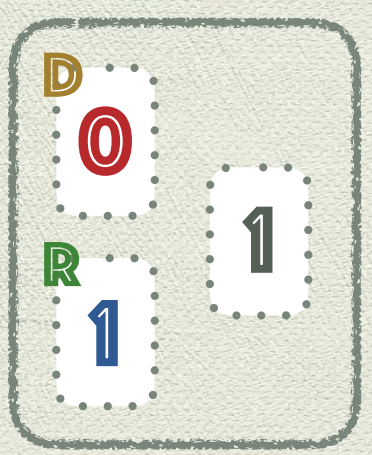
R 1

$b = (0\ 1\ 0)_2$

プロトコルの実行例：3rd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$



$b = (0\ 1\ 0)_2$

プロトコルの実行例：3rd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

スワップ済み
そのままでOK

D 0

R 1

1

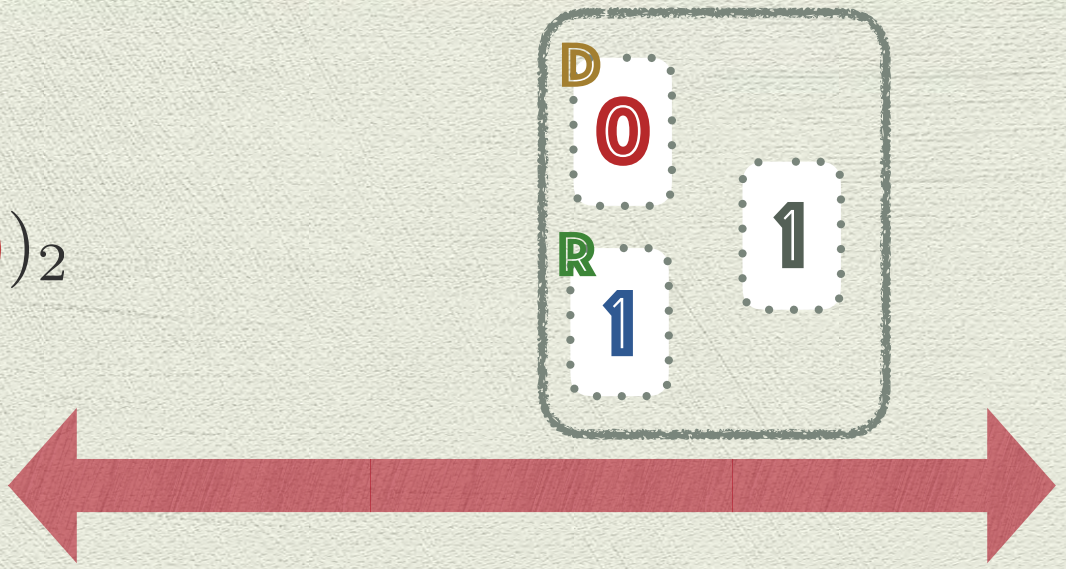
$a = (0\ 0\ 0)_2$

$b = (0\ 1\ 0)_2$

プロトコルの実行例：3rd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

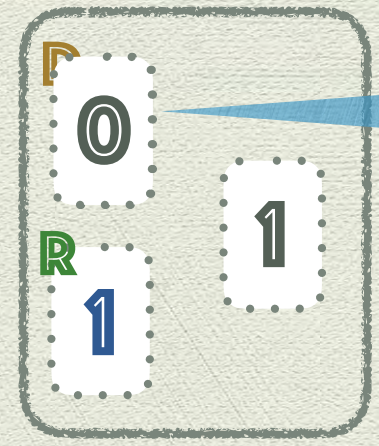


$b = (0\ 1\ 0)_2$

プロトコルの実行例：3rd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]

$a = (0\ 0\ 0)_2$

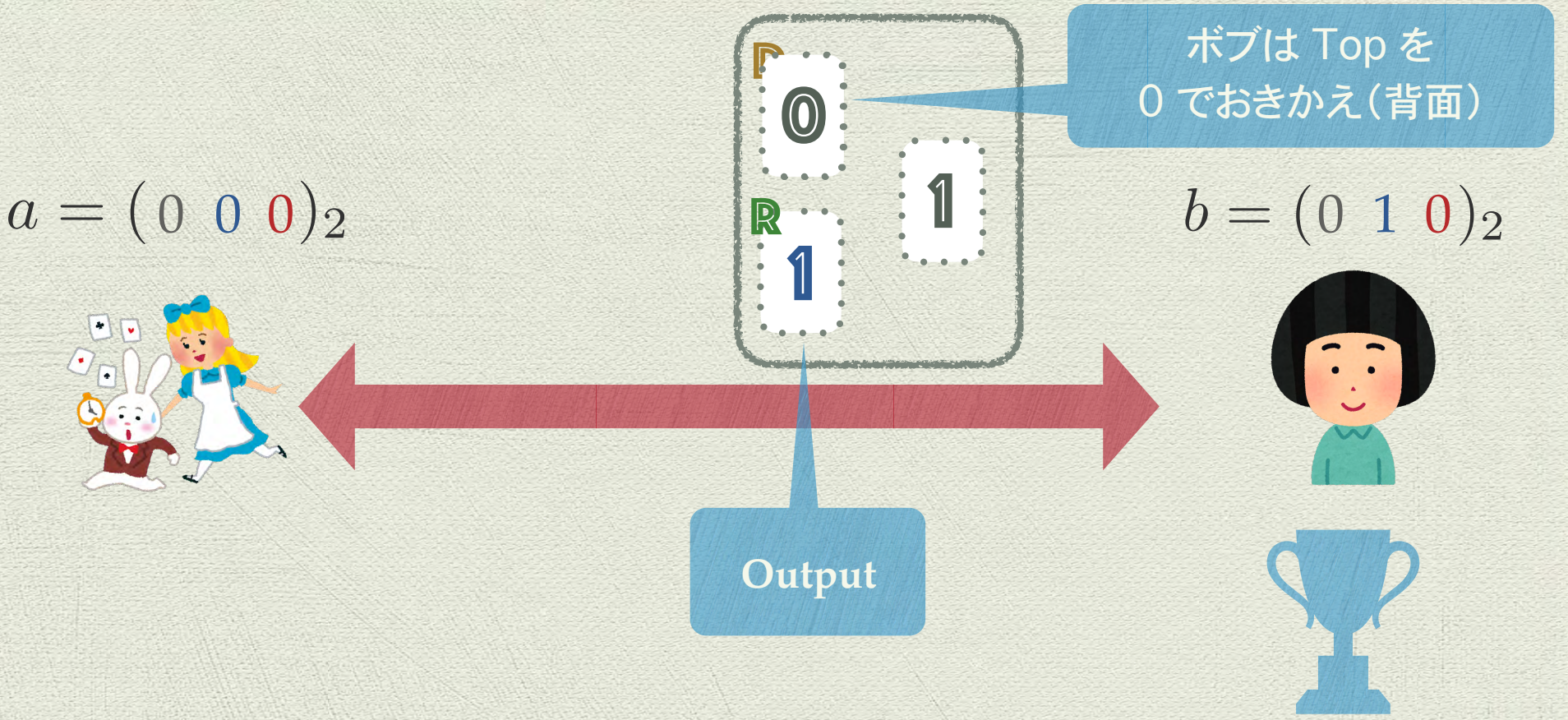


ボブは Top を
0 でおきかえ（背面）

$b = (0\ 1\ 0)_2$

プロトコルの実行例：3rd Round

[Nakai-Misawa-Tokushige-Iwamoto-Ohta, CANS2016]



この話
嘘つき島と同じだということに
気がつきましたか？

整理：『嘘つき村問題』との関係

この道が「正直村」に行く場合：

[Q] この道はあなたの村に行きますか？

	正直村の住人か	He says
正直村の人	True	Yes
嘘つき村の	False	Yes

$a_i \neq b_i$ である場合

[Q] "Record" が置き換えられるか？

Top/Bottom strategy

	$\tilde{a}_i \neq b_i$	Record が置き換わる
a_i を送る	True (Top = Rec.)	Yes (Top が置き換わる)
$\overline{a_i}$ を送る	False (Bot. = Rec.)	Yes (Bottom が換わる)

まとめ

- 『金持ち比べ問題』に対するカードベース暗号プロトコルの提案
- 興味深い関係
  - セキュリティ (マルチパーティ計算)
  - 論理 (『嘘つき村問題』)
- 効率性ほか（省略）
  - 先行研究より以下の指標で優れていることが分かっている
    - 使用するカード枚数
    - 通信回数

おわり